Federal Aviation Administration

Safety Assurance Briefing

Presented to: Verification and Validation Summit

By: Mark DeNicuolo, Manager, Safety Assurance

Date: October 23, 2008

Aligning Safety Assurance Assessments with SMS

- Observation from Customers/Stakeholders:
  - IOT&E issues definitions are different from the risk ratings in the SMS Manual.
  - There is a clear desire for consistency in terminology and definitions.
- Therefore the IOT&E process was enhanced to incorporate SMS terminology and definitions.

Aligning Assessments with SMS

- Risk Ratings:
  - Replaced old 3X3 High, Medium, Low issue rating with SMS 5X5 matrix.

Severity Likelihood	No Safety Effect 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A	L	M	H	H	H
Probable B	L	M	H	H	H
Remote C	L	L	M	H	H
Extremely Remote D	L	L	L	M	H
Extremely Improbable E	L	L	L	L	H* M

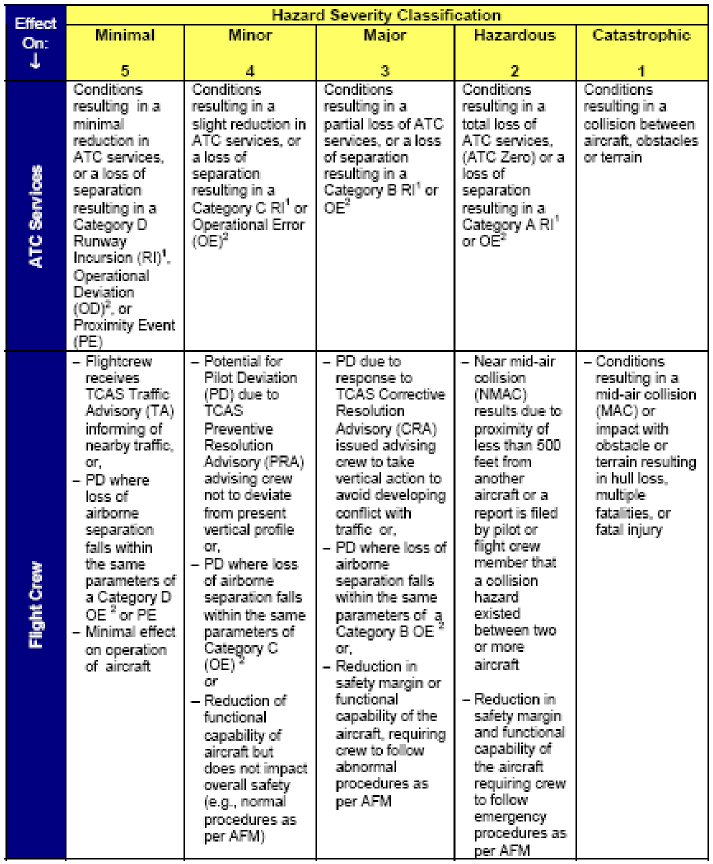
🟥 High Risk
🟨 Medium Risk
🟩 Low Risk

* Unacceptable with Single Point and/or Common Cause Failures

Aligning Assessments with SMS

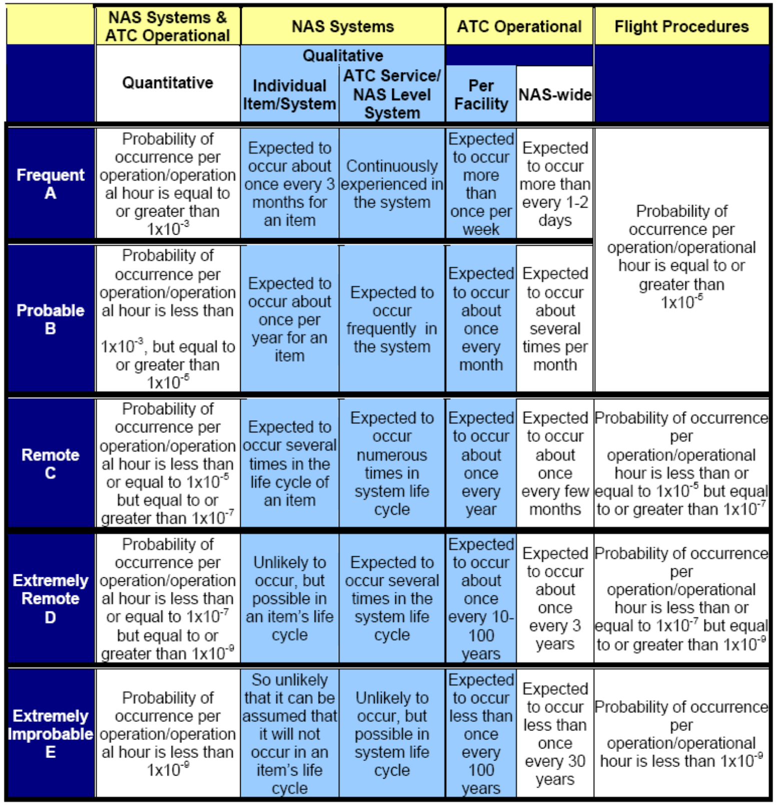
- Incorporate Severity and Likelihood analysis in issue rating determination

Table 3.3: Severity Definitions



Effect On: ↓	Hazard Severity Classification				
	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
ATC Services	Conditions resulting in a minimal reduction in ATC services, or a loss of separation resulting in a Category D Runway Incursion (RI)[1], Operational Deviation (OD)[2], or Proximity Event (PE)	Conditions resulting in a slight reduction in ATC services, or a loss of separation resulting in a Category C RI[1] or Operational Error (OE)[2]	Conditions resulting in a partial loss of ATC services, or a loss of separation resulting in a Category B RI[1] or OE[2]	Conditions resulting in a total loss of ATC services, (ATC Zero) or a loss of separation resulting in a Category A RI[1] or OE[2]	Conditions resulting in a collision between aircraft, obstacles or terrain
Flight Crew	– Flightcrew receives TCAS Traffic Advisory (TA) informing of nearby traffic, or, – PD where loss of airborne separation falls within the same parameters of a Category D OE [2] or PE – Minimal effect on operation of aircraft	– Potential for Pilot Deviation (PD) due to TCAS Preventive Resolution Advisory (PRA) advising crew not to deviate from present vertical profile or, – PD where loss of airborne separation falls within the same parameters of Category C (OE) [2] or – Reduction of functional capability of aircraft but does not impact overall safety (e.g., normal procedures as per AFM)	– PD due to response to TCAS Corrective Resolution Advisory (CRA) issued advising crew to take vertical action to avoid developing conflict with traffic or, – PD where loss of airborne separation falls within the same parameters of a Category B OE [2] or, – Reduction in safety margin or functional capability of the aircraft, requiring crew to follow abnormal procedures as per AFM	– Near mid-air collision (NMAC) results due to proximity of less than 500 feet from another aircraft or a report is filed by pilot or flight crew member that a collision hazard existed between two or more aircraft – Reduction in safety margin and functional capability of the aircraft requiring crew to follow emergency procedures as per AFM	– Conditions resulting in a mid-air collision (MAC) or impact with obstacle or terrain resulting in hull loss, multiple fatalities, or fatal injury

Table 3.4: Likelihood Definitions

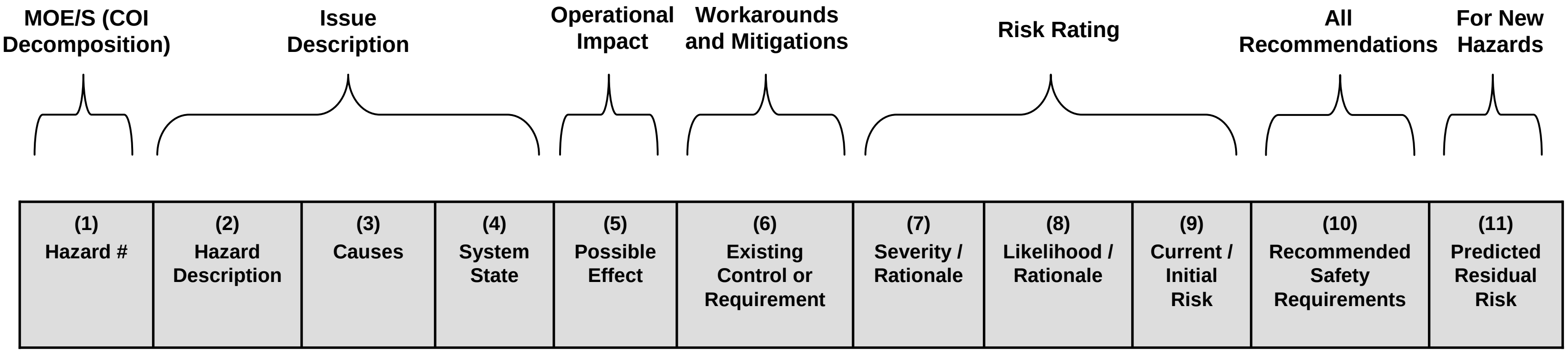


	NAS Systems & ATC Operational	NAS Systems		ATC Operational		Flight Procedures
	Quantitative	Qualitative				
		Individual Item/System	ATC Service/ NAS Level System	Per Facility	NAS-wide	
Frequent A	Probability of occurrence per operation/operational hour is equal to or greater than 1x10^{-3}	Expected to occur about once every 3 months for an item	Continuously experienced in the system	Expected to occur more than once per week	Expected to occur more than every 1-2 days	Probability of occurrence per operation/operational hour is equal to or greater than 1x10^{-5}
Probable B	Probability of occurrence per operation/operational hour is less than 1x10^{-3}, but equal to or greater than 1x10^{-5}	Expected to occur about once per year for an item	Expected to occur frequently in the system	Expected to occur about once every month	Expected to occur about several times per month	
Remote C	Probability of occurrence per operation/operational hour is less than or equal to 1x10^{-5} but equal to or greater than 1x10^{-7}	Expected to occur several times in the life cycle of an item	Expected to occur numerous times in system life cycle	Expected to occur about once every year	Expected to occur about once every few months	Probability of occurrence per operation/operational hour is less than or equal to 1x10^{-5} but equal to or greater than 1x10^{-7}
Extremely Remote D	Probability of occurrence per operation/operational hour is less than or equal to 1x10^{-7} but equal to or greater than 1x10^{-9}	Unlikely to occur, but possible in an item's life cycle	Expected to occur several times in the system life cycle	Expected to occur about once every 10-100 years	Expected to occur about once every 3 years	Probability of occurrence per operation/operational hour is less than or equal to 1x10^{-7} but equal to or greater than 1x10^{-9}
Extremely Improbable E	Probability of occurrence per operation/operational hour is less than 1x10^{-9}	So unlikely that it can be assumed that it will not occur in an item's life cycle	Unlikely to occur, but possible in system life cycle	Expected to occur less than once every 100 years	Expected to occur less than once every 30 years	Probability of occurrence per operation/operational hour is less than 1x10^{-9}

Aligning Assessments with SMS

- Follow the SRM Safety Analysis Phases:

IOT&E



MOE/S (COI Decomposition)	Issue Description			Operational Impact	Workarounds and Mitigations	Risk Rating			All Recommendations	For New Hazards
(1) Hazard #	(2) Hazard Description	(3) Causes	(4) System State	(5) Possible Effect	(6) Existing Control or Requirement	(7) Severity / Rationale	(8) Likelihood / Rationale	(9) Current / Initial Risk	(10) Recommended Safety Requirements	(11) Predicted Residual Risk

SRM

- Analysis revealed we were already including these phases in IOT&E process.

Aligning Assessments with SMS

- Expectations
  - Operational issues usually will have safety impact.
  - The SRM severity and likelihood definitions account for situations where the effect on safety is marginal but there is an impact to operations.
  - Therefore the SRM definitions can be used for all issues and there is no need for another classification system for operational issues.
  - However, since the SRM definitions are less severe for instances where operations are impacted but the safety risk is marginal, the team expects fewer High risk issues than in the past.

Aligning Assessments with SMS

- Conclusion so far…
  - On the surface it appeared to be a major change…in effect the changes were minimal.
  - IOT&E Team members need some basic SRM training.
  - Operational issues can be effectively categorized using the SRM definitions, however they may not be assessed as High risk.
- Recently finished preliminary Independent Safety Assessment Report for ADS-B using new process and definitions.
  - IOT&E terms and definitions are seamless with SMS/SRM.

Seamless V&V

- **Similar V&V issue identification terms and definitions throughout the agency would support:**
  - A formalized and consistent test structure and
  - Transparency of information

Test Standards Board

- Formalized structure
- Clearly defined role
- Transparency of information
- Consider broadening role to *ensure* conformity

Visit Our Website

Go to: http://atoexperience.faa.gov/safety/

Coming Soon

Information on the 2nd Annual SMS Summit:

"SMS: Soaring Into The Next Generation"

June 2-4, Dallas, TX